

REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-6 and 13-24 are pending. Claims 1, 2 and 14 are amended to at least correct minor grammatical errors and to conform the claims according to commonly accepted US patent practice. New claims 21-24 have been added to secure an appropriate scope of protection to which Applicants are believed entitled.

Independent claim 1 is amended to recite a method of detecting critical file changes, comprising, *inter alia*, reading an event representing at least one system call, “wherein the event is a kernel audit record read from an intrusion detection data source (IDDS). . . .”

Independent claim 14 is amended to recite a system for detecting critical file changes, comprising, *inter alia*, a memory storing instructions which, when executed by the processor, cause the processor to “read an event from an intrusion detection data source (IDDS), wherein the event is a kernel audit record. . . .” Support for the amendments to the claims is believed to be found at at least page 4, lines 7-18. No new matter has been added.

Amended and unamended claims 1-6 and 13-20 are not anticipated by Moran (US 6,647,400)

The 35 U.S.C. §102(e) rejection of claims 1-6 and 13-20 over Moran is respectfully traversed.

A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Moran fails to anticipate the subject matter of amended claim 1 because Moran fails to disclose at least a method of detecting critical file changes, comprising “reading an event representing at least one system call, wherein an event is a kernel audit record read from an intrusion detection data source (IDDS). . . .”

Based on at least the foregoing reason, Moran does not disclose, teach or suggest each limitation recited in amended claim 1. Therefore, claim 1 is patentable over Moran, and the rejection is respectfully requested to be withdrawn.

Claims 2-6 depend, either directly or indirectly, from claim 1, include further limitations, and are patentable over *Moran* for at least the reasons advanced above with respect to claim 1. The rejection of claims 2-6 should be withdrawn.

Amended claim 14 is patentable over Moran for at least reasons similar to those advanced above with respect to claim 1 and the rejection is respectfully requested to be withdrawn.

Claims 15-20 depend, either directly or indirectly, from claim 14, include further limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 14. Withdrawal of the rejection over Moran is respectfully requested.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claim 1-6 and 13-22 are earnestly solicited.

Should the Patent and Trademark Office (PTO) believe that anything further would be desirable in order to place this application in even better condition for allowance, the PTO is invited to contact the undersigned at the telephone number set forth below.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

Mark Crosbie

A handwritten signature in dark ink, appearing to read "Randy A. Noranbrock". The signature is fluid and cursive, with the first name "Randy" being more prominent.

Randy A. Noranbrock
Registration No. 42,940
Telephone: (703) 684-1111

HEWLETT-PACKARD COMPANY

IP Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80528-9599
Telephone: (970) 898-7057
Facsimile: 281-926-7212
Date: **May 21, 2007**
RAN/ERM